

In the Claims

1
2 1. (currently amended) A printer device comprising:
3 a data input device for receiving an encrypted digital document file;
4 a decryption algorithm for decrypting said received document file;
5 a controller for controlling printing of an image of data contained in said
6 received document file, wherein said controller operates to read a quantity
7 permission data content of said document file, said quantity permission data
8 specifying a number of authorized copies of said document file to be printed; and
9 a printer mechanism for printing a physical copy of said document file,
10 wherein said controller operates to control printing of a predetermined
11 quantity of said physical copy, and after printing of said physical copy,
12 automatically deletes said electronic document file from said memory.

13
14 2. (original) The printer device as claimed in claim 1, further comprising a
15 decryption key locally stored in said printer device.

16
17 3. (original) The printer device as claimed in claim 1, comprising a
18 network interface for receiving said encrypted digital document file over a
19 network.
20
21
22
23
24
25

1 4. (original) The printer device as claimed in claim 1, wherein said
2 controller stores a unique device identification data uniquely identifying said
3 printer device, said controller operating to:

4 compare a received unique identifier data contained in said received
5 document file with said stored unique device identifier; and

6 if said received unique device identifier data differs from said stored unique
7 device identifier data, delete said document file.

8
9 5. (original) The printer device as claimed in claim 1, wherein said
10 controller stores a unique device identification data uniquely identifying said
11 printer device, said controller operating to:

12 compare a received unique identifier data contained in said received
13 document file with said stored unique device identifier; and

14 if said received document identification data is identical to said received
15 unique device identifier data, control said print mechanism to print at least one
16 said physical copy of said document file.

17
18 6. (currently amended) The printer device as claimed in claim 1, wherein:

19 ~~said controller operates to read a quantity permission data content of said~~
20 ~~document file, said quantity permission data specifying a number of authorised~~
21 ~~copies of said document file to be printed; and~~

22 said controller controls said printer mechanism such that said permitted
23 quantity of physical copies of said document file are printed.

1 7. (original) The printer device as claimed in claim 1, wherein:
2 said controller operates to generate a confirmation message confirming
3 receipt of said document file.

4
5 8. (original) The printer device as claimed in claim 1, wherein;
6 said controller operates to generate a confirmation message confirming
7 receipt of said document file;

8 said confirmation message comprises a time and date data, specifying a
9 time and date of receipt of said document file and a number of copies printed data,
10 specifying a number of copies of said document file physically printed by said
11 print mechanism.

1 9. (currently amended) A printer device comprising:

2 a data input device for receiving an encrypted digital document file;

3 a decryption algorithm for decrypting said received document file;

4 a controller for controlling printing of an image of data contained in said
5 received ~~documents~~ document file, wherein said controller operates to read a
6 quantity permission data content of said document file, said quantity permission
7 data specifying a number of authorized copies of said document file to be printed;
8 and

9 a printer mechanism for printing a physical copy of said document file,
10 wherein said controller operates to check a unique device identification data
11 contained in said document file with a stored unique device identification data of
12 said printer device, and provided a successful match is found, print said physical
13 copy of said document file; and

14 if said received unique device identifier differs from said stored unique
15 device identifier data, said controller operates to delete said document file without
16 printing a physical copy of said document file.

17
18
19
20
21
22
23
24
25

1 10. (currently amended) A computer entity configured for sending secure
2 encrypted document files, said computer entity comprising:

3 a data processor;

4 a memory;

5 an encryption algorithm capable of encrypting a document file;

6 a device selector for selecting a said uniquely identifiable recipient device;

7 a file selector for selecting a document file;

8 a stored list of a set of ~~authorised~~authorized recipient devices, each said
9 recipient device identified by a unique device identifier data inaccessibly
10 embedded within said computer entity;

11 wherein said computer entity operates to:

12 select at least one document file;

13 select at least one said uniquely identifiable recipient device to send
14 said document ~~to~~; to;

15 encrypt said document files; and

16 address said at least one document file to said selected uniquely
17 identified recipient ~~device~~; device; and

18 a user interface capable of displaying a history list of document files sent,
19 said history list comprising:

20 data describing a document file sent;

21 data describing at least one said recipient device to which said
22 document file has been sent; and

23 data describing a number of copies of documents said recipient
24 device is authorized to print from said received document file.
25

1
2 11. (original) The computer entity as claimed in claim 10, further
3 comprising:

4 a network interface capable of sending said document file over a network to
5 said selected recipient device.
6

7 12. (currently amended) The computer entity as claimed in claim 10,
8 wherein:

9 said controller said controller operates to read a quantity permission data
10 content of said document file, said quantity permission data specifying a number
11 of authorized copies of said document file to be printed; and

12 said controller controls said printer mechanism such that said permitted
13 quantity of physical copies of said document file are printed.

14 ~~further comprising a user interface capable of displaying a history list of~~
15 ~~document files sent, said history list comprising:~~

16 ~~data describing a document file sent;~~

17 ~~data describing at least one said recipient device to which said document~~
18 ~~file has been sent;~~

19 ~~data describing a number of copies of documents said recipient device is~~
20 ~~authorised to print from said received document file.~~

21
22 13. (original) The computer entity as claimed in claim 10, wherein said
23 user interface further displays:

24 data describing an encryption method used for sending said document.
25

1
2 14. (original) The computer entity as claimed in claim 10, wherein said
3 user interface displays:

4 an acknowledgement message data describing receipt of said document file
5 by a said recipient device.
6

7 15. (currently amended) A distributed secure document printing system,
8 said system comprising:

9 at least one sending computer entity, capable of sending an encrypted
10 electronic document file, said document file having an encrypted data content, and
11 a unique device identifier data identifying a recipient printer device to which said
12 document file is intended to be printed by; and

13 at least one recipient printer device, said recipient printer device capable of
14 receiving said encrypted document file, establishing that said document file is
15 intended for said recipient printer device, decrypting and printing said document
16 file, and automatically deleting said electronic document file after printing a
17 physical copy of a document from said document file[.];

18 wherein said recipient printer device is configured to send a confirmation
19 message back to said sending computer entity, confirming receipt of said
20 document file, and confirming printing of a specified permitted number of copies
21 of said document file.
22
23
24
25

1 16. (original) The system as claimed in claim 15, wherein said recipient
2 printer device is capable of reading a permitted quantity data content of said
3 document file; and

4 said recipient printer device operates for printing a number of physical
5 copies of said document file, corresponding to said permitted quantity data.

6
7 17. (cancel)
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

1 18. (currently amended) A method of securely communicating an
2 electronic document file over a network, said method comprising the steps of:

3 encrypting said document file;

4 specifying a recipient device for sending said document file to, said
5 recipient device being uniquely identifiable by a unique device identifier data;

6 attaching said unique identifier data to said document file;

7 sending said document file in encrypted format to said intended recipient
8 device;

9 receiving said transmitted document file and decrypting said document file;

10 reading said unique device identifier data of said document file;

11 if said unique device identifier data of said document file corresponds to a
12 unique device identifier data of said recipient device, printing a physical copy of
13 said document file; ~~and~~

14 if said unique device identifier data of said document file does not
15 correspond with said unique device identifier data of said recipient device,
16 deleting said received document file without printing a physical copy of said
17 document file[.]; and

18 sending, from said recipient device, a confirmation message back to said
19 sending computer entity, confirming receipt of said document file, and confirming
20 printing of a specified permitted number of copies of said document file.

1 19. (original) The method as claimed in claim 18, further comprising the
2 step of:

3 after printing said physical copy, deleting said electronic document file
4 from said recipient device;

5
6 20. (original) The method as claimed in claim 18, further comprising the
7 step of:

8 specifying a permitted quantity of physical copies of said document file to
9 be printed; and

10 printing said permitted number of copies of said document file.
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

1 21. (currently amended) A method of secure printing of a received
2 document file, said method comprising the steps of:

3 receiving said document file in encrypted format at a receiving device;

4 decrypting said document file;

5 reading a unique device identifier data identifying a recipient device for
6 which said document file is intended;

7 comparing said unique device identifier data with a locally stored device
8 identifier data stored at said receiving device;

9 if said received unique device identifier data corresponds with said locally
10 stored device identifier data, printing at least one physical copy of said document
11 file;

12 if said received unique device identifier data differs from said stored unique
13 device identifier data, deleting said document file[.]; and

14 sending, from said recipient device, a confirmation message back to said
15 sending computer entity, confirming receipt of said document file, and confirming
16 printing of a specified permitted number of copies of said document file.

17
18 22. (original) The method as claimed in claim 21, further comprising the
19 step of:

20 deleting said electronic document file, after printing said physical copy of
21 said document file.

1 23. (original) The method as claimed in claim 21, further comprising the
2 step of:

3 reading a permitted quantity data describing a permitted quantity of copies
4 of said document file; and

5 printing said permitted quantity of copies of said document file.

6
7 24. (original) The method as claimed in claim 21, wherein said document
8 file, after decryption is prevented from being viewed on a visual display device
9 prior to printing.

10
11 25. (original) The method as claimed in claim 21, wherein said document
12 file is received via an intermediary carrier device having data storage capability.

13
14 26. (currently amended) A method of sending a document file for printing
15 by a specified ~~authorised~~authorized recipient printing device, said method
16 comprising the steps of:

17 selecting a content of said document file;

18 encrypting said content;

19 attaching a unique device identifier data, identifying a recipient device to
20 which said document file is to be sent;~~and~~

21 sending said document file to said recipient device[[]]; and

22 adding a permitted quantity data to said document file, said permitted
23 quantity data specifying a permitted number of copies of said document file which
24 can be printed.

1
2 27. (cancel)

3
4 28. (original) The method as claim in claim 26, further comprising the
5 steps of:

6 storing a document history data, said document history data specifying for
7 said document file:

8 a list of at least one recipient device to which said document file may
9 be sent;

10 a number of permitted copies of said document file which are
11 permitted to be printed by each said recipient device.

1 29. (currently amended) A computer entity comprising a data processor, a
2 data storage device, a printer port, and having an attached printer device, said
3 computer entity comprising:

4 a module for decrypting an encrypted document file;

5 a unique device identifier for identifying said computer entity;

6 wherein said computer entity operates to:

7 receive a document file in encrypted format;

8 decrypt said document;

9 extract a unique device identifier data from said document;

10 compare said extracted unique identifier data with said unique
11 device identifier of said computer entity;

12 if a match is found between said received unique device identifier
13 data of said document and said unique identifier of said computer entity, send a
14 said document file for printing by said attached printer device; and

15 after sending said document to said printer device, delete said
16 document file from said computer entity[[]]; and

17 adding a permitted quantity data to said document file, said permitted
18 quantity data specifying a permitted number of copies of said document file which
19 can be printed.

1 30. (currently amended) A method of secure printing of a received
2 document file, said method comprising the steps of:

3 receiving said document file in encrypted format;

4 reading a unique device identifier data identifying a recipient device for
5 which said document file is intended;

6 comparing said unique device identifier data with a locally stored identifier
7 data corresponding to a local computer entity device;

8 if said locally stored identifier data differs from said unique device
9 identifier data identifying said recipient device for which said document file is
10 intended, deleting said document file without printing any physical copies of said
11 document file[.]; and

12 printing a number of physical copies of said document file, corresponding
13 to a permitted quantity defined in said document file.

1 31. (currently amended) A method of secure printing of a received
2 document file, said method comprising the steps of:
3 receiving said document file in encrypted format;
4 reading a unique device identifier data identifying a recipient device for
5 which said document file is intended;
6 comparing said unique device identifier data with a locally stored device
7 identifier data;
8 reading a permitted quantity data describing a permitted quantity of copies
9 of said document file; and
10 if said received unique device identifier data corresponds with said locally
11 stored device identifier data, printing said permitted quantity of copies of said
12 document file[.]; and
13 printing a number of physical copies of said document file, corresponding
14 to a permitted quantity defined in said document file.
15
16
17
18
19
20
21
22
23
24
25

1 32. (currently amended) A printer device comprising:
2 a data input device for receiving an encrypted digital document file;
3 a decryption algorithm for decrypting said received document file;
4 a controller for controlling printing of an image of data contained in said
5 received document file; and
6 a printer mechanism for printing a physical copy of said document file,
7 wherein said printer device locally stores a decryption key for operating
8 said decryption algorithm to decrypt said received document file[.]; and
9 wherein said printer device is configured to send a confirmation message
10 back to said sending computer entity, confirming receipt of said document file,
11 and confirming printing of a specified permitted number of copies of said
12 document file.
13
14
15
16
17
18
19
20
21
22
23
24
25

1 33. (currently amended) A printer device comprising:
2 a data input device for receiving a digital document file;
3 a controller for controlling printing of an image of data contained in said
4 received document file; and
5 a printer mechanism for printing a physical copy of said document file,
6 wherein said controller operates to compare a received unique identifier
7 data contained in said received document file with a locally stored unique device
8 identifier data stored at said printer device and operates to control printing of a
9 predetermined quantity of said physical copy, wherein said predetermined quantity
10 is specified in said received document file;
11 if said received unique identifier data matches said stored unique device
12 identifier, control printing of at least one said physical copy of said document file;
13 and
14 if said received unique identifier data contained the said received document
15 file does not match said stored unique device identifier data, to inhibit printing of
16 any physical copies of said document file.
17

18 34. (cancel)
19
20
21
22
23
24
25

1 35. (currently amended) A printer device comprising:
2 a data input device for receiving an encrypted digital document file;
3 a decryption algorithm for decrypting said received document files; a
4 controller for controlling printing of an image of data contained in said received
5 document file; and
6 a printer mechanism for printing a physical copy of said document file,
7 wherein a decryption key is stored locally in said printer device for
8 operating said decryption algorithm to decrypt said received document files;
9 said controller operates to compare a received unique identifier data
10 contained in said received document file with a locally stored unique device
11 identifier data stored at said printer device;
12 if said received unique identifier data matches said stored unique device
13 identifier, control printing of at least one said physical copy of said document file;
14 and
15 if said received unique identifier data contained the said received document
16 file does not match said stored unique device identifier data, to inhibit decryption
17 of said document file and inhibit printing of any physical copies of said document
18 file[.];
19 wherein said printer device is configured to send a confirmation message
20 back to said sending computer entity, confirming receipt of said document file,
21 and confirming printing of a specified permitted number of copies of said
22 document file.
23
24
25